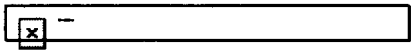
[0042] It is not necessary to accumulate the password itself with information centre equipment 3, and by the method of the example of **** 2, since it is only an encryption password, the security nature of information centre equipment 3 becomes very high.
[0043] Next, the operations sequence of the 3rd example at the time of receiving information is explained to a terminal unit 2 based on the flow chart of drawing 10 from information centre equipment 3. The 3rd example is the approach of holding the password of each terminal unit 2 to information centre equipment 3, and collating a password with it by the information centre equipment 3 side. Here, the contents of the user information storage section 31 are the same as the contents of drawing 4 .
[0044] It connects with information centre equipment 3, the user identification number extracted from the security information are recording section 11 in the card section 1 is transmitted, and a terminal unit 2 requires digital information (SD1).
[0045] With information centre equipment 3, the random number R of arbitration is generated (SD2), and it transmits to a terminal unit 2 (SD3). As it signs with the user signature key Di in the signature generation section 25 (SD4) and the password entered from the input section 23 is further shown in the following (11) types in the open encryption section 26, an encryption password and said received random number R verify using the center verification key Cp (SD5), and in the terminal unit 2 which received the random number R from information centre equipment 3, it transmits to information centre equipment 3 (SD6).
[0046]
[Equation 11]

Then, in information centre equipment 3, by the signature generation section 34, it signs using the center signature key Cs to said received encryption information (SD7), and an encryption password is further verified with the user verification key Ei (SD8). Next, the random number and password which were obtained are collated with said transmitted random number and the password in the user information storage section 31 by the collating section 38, respectively (SD9). As a result of this collating, when either is an inequality, the circuit of a terminal unit 2 and information centre equipment 3 is cut (SD10). In coincidence of a random number and a password A session key is generated in the session key generation section 33 (SD11), and it verifies in the verification section 36 using the user verification key Ei (SD12), and

transmits to a terminal unit 2 (SD13).
[0047] Then, with a terminal unit 2, as shown in the following (12) types, after signing said received encryption session key with the user signature key Di in the signature generation section 25 (SD14), in the open encryption section 26, this signature information is enciphered with a center verification key (SD15), and it transmits to information centre equipment 3 (SD16).
[0048]
[Equation 12]



In addition, since the processing of SD17-SD25 after this (procedure which performs session key collating and information body delivery, and accumulates receipt information in a terminal unit with information centre equipment) is the same as that of the procedure of SA14-SA22 in the 1st example explained previously, the explanation is omitted.
[0049] As mentioned above, according to the 1st thru/or the 3rd example, only the normal user who received information can offer the digital information communication system using the information accumulated in information centre equipment 3 using the card section 1, and the protection of an informational copyright holder of him is attained.
[0050] Next, the 4th example of this invention is explained based on drawing 11 . The 4th example shows how to use said receipt information from the terminal unit in another airraid from which the accepting-station equipment which received information differs.
[0051] In drawing 11 , a terminal unit A shows the equipment which received digital information from the information centre equipment 3 in drawing 1 , and was accumulated in the information storage section 28, and is a terminal unit which is going to use the digital information which a terminal unit A has a terminal unit B in another airraid, and is accumulated in the terminal unit A.
[0052] Next, the operations sequence of the 4th example which consists of the above-mentioned configuration is explained based on the flow chart shown in drawing 12 . First, the card section 1 which the user who wants to use digital information owns is connected to a terminal unit B (SE1). Subsequently, a terminal unit B is connected to a terminal unit A through the communications control section 20 (SE2), the encryption password PWi corresponding to information to use in the information storage section 28 of a terminal unit A is extracted (SE3), and it transmits to a terminal unit B (SE4). In a terminal unit B, the encryption password received from the terminal unit A with the card

private key Ki extracted from the security information are recording section 11 of the card section 1 is decoded in common use encryption / decode section 27 (SE5). Then, by the collating section 22 The decoded password and the password entered from the input section 23 are collated (SE6), when the result of this collating is an inequality, informational use is forbidden, and a circuit with a terminal unit A is cut (SE7). Moreover, when said password is in agreement as a result of collating, in a terminal unit A, the information body enciphered with the encryption session key and this session key is extracted from the information storage section 28 (SE8), and it transmits to a terminal unit B (SE9).

[0053] Then, in a terminal unit B, after decoding the received encryption session key with the card private key Ki extracted from the security information are recording section 11 of the card section 1 (SE10), the information body enciphered with this session key is decoded (SE11), and this decoded information body is outputted and used from the information output section 29 (SE12).

[0054] In addition, although it is the approach of using the digital information which the example of **** 4 accessed its own terminal unit A from other terminal units B, and was received to the terminal unit A before, it cannot be overemphasized that direct information centre equipment 3 is accessed from other terminal units B, and new digital information can be received and used.

[0055] Next, the example which has the set of two or more card sections 1 as the 5th example of this invention is explained based on drawing 13 . The card private key Ki and the center verification key Cs are the same, and an information provider publishes two or more card sections 1 from which the user signature key Di differs in a user identification number UIDi list as shown in drawing 13 . For example, it is the card section 1 published for the group who closed the section in a family and a firm etc. As for the digital information which either of the group constituents who hold this card section 1 received by this, anyone, a group constituent, can offer an available environment free anywhere. In that case, if the information tariff in the case of digital information reception is changed by several card ball to publish and the group configuration number, the profits of a copyright person and an information provider will not be spoiled.

[0056]

[Effect of the Invention] As explained above, according to the digital information communication system of this invention according to claim 1 After receiving digital information using the card section which

recorded a user's identification information, Since information is made available after setting and accumulating the enciphered individual humanity news and an information decode key and collating individual humanity news by said user's card section in the case of information use, in case it accumulates in a terminal unit Only the digital information user of normal can use this information, and can prevent an informational unauthorized use. Thereby, while being able to prevent literary piracy, the profits of a copyright person and an information provider are not spoiled. Moreover, a user's whereabouts and the whereabouts of digital information can offer the system which can be used wherever it may be in, and have big effectiveness for a user's convenience for protection of copyright. Furthermore, it is not dependent on an information provider and a terminal unit has the big advantage which manufactures freely and can be sold to a user.

[0057] Moreover, according to claim 2, in addition to the above-mentioned effectiveness, a card private key and a center verification key be the same, and when an information provider publish two or more card sections from which a user signature key differ in a user identification number list, they have the big advantage which can offer a system convenient for both by the side of a user and an information provider (expansion of the use number) (large sum collection of an information tariff).

[0058] Moreover, according to the digital information correspondence procedure according to claim 3 to 5 After receiving digital information using the card section which recorded a user's identification information, Since information is made available after setting and accumulating the enciphered individual humanity news and an information decode key and collating individual humanity news by said user's card section in the case of information use, in case it accumulates in a terminal unit Only the digital information user of normal can use this information, and can prevent an informational unauthorized use. Thereby, while being able to prevent literary piracy, the profits of a copyright person and an information provider are not spoiled.

[0059] Furthermore, it is not necessary to accumulate a password in an information centre equipment side, and, according to the digital information correspondence procedure according to claim 4, in addition to the above-mentioned effectiveness, the security nature by the side of information centre equipment can be raised very much.

[0060] Moreover, according to the digital information correspondence procedure according to claim 6, the card section which recorded a user's identification information is used. Since information is made available

after receiving digital information, setting and accumulating the enciphered individual humanity news and an information decode key and collating individual humanity news by said user's card section in the case of information use in case it accumulates in a terminal unit Only the digital information user of normal can use this information, and can prevent an informational unauthorized use. Thereby, while being able to prevent literary piracy, the profits of a copyright person and an information provider are not spoiled. Furthermore, since information can be taken out and used from terminal unit with the another terminal unit in which information carries out the whereabouts, the big effectiveness for a user's convenience for protection of copyright is done so.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram showing the digital information communication system of the 1st example of this invention
[Drawing 2] The flow chart which shows reception of the information in the 1st example, and the operations sequence to are recording
[Drawing 3] Drawing showing the contents of information of the security information are recording section of card circles in the 1st example
[Drawing 4] Drawing showing the contents of information of the user information storage section in the 1st example
[Drawing 5] Drawing showing the contents of information of the center signature key are recording section in the 1st example
[Drawing 6] Drawing showing the contents of information of the information storage section in the 1st example
[Drawing 7] The flow chart which shows the procedure in the case of using the information received with the terminal unit in the 1st example
[Drawing 8] The flow chart which shows reception of the information in the 2nd example of this invention, and the operations sequence to are recording
[Drawing 9] Drawing showing the contents of information of the user information storage section used in the 2nd example
[Drawing 10] The flow chart which shows reception of the information in the 3rd example of this invention, and the operations sequence to are recording
[Drawing 11] 4th operation instantiation ******* of this invention

[Drawing 12] The flow chart which shows the information use procedure in the 4th example

[Drawing 13] Drawing explaining two or more card sections which can be set in the 5th example of this invention

[Description of Notations]

1 [-- Security information are recording section,] -- The card section, 2 -- A terminal unit, 3 -- Information centre equipment, 11 20 [-- The input section, 24 / -- Session key extract section,] -- The communications control section, 21 -- The verification section, 22 -- The collating section, 23 25 -- The signature generation section, 26 -- The open encryption section, 27 -- Common use encryption / decode section, 28 [-- The user information storage section, 32 / -- The center signature key are recording section, 36 / -- The verification section, 37 / -- The signature information storage section, 38 / -- The collating section, 39 / -- The encryption section, 40 / -- Information storage section.] -- The information storage section, 29 -- The information output section, 30 -- The communications control section, 31

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－288519

(43)公開日　平成７年(1995)10月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｇ０９Ｃ	1/00		9364－5Ｌ			
				Ｈ０４Ｌ	9/02	Ｚ

審査請求　未請求　請求項の数６　ＯＬ　（全 20 頁）

(21)出願番号　特願平6－80570

(22)出願日　平成６年(1994)４月19日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　山中　喜義
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　神田　雅透
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　小柳津　育郎
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　吉田　精孝

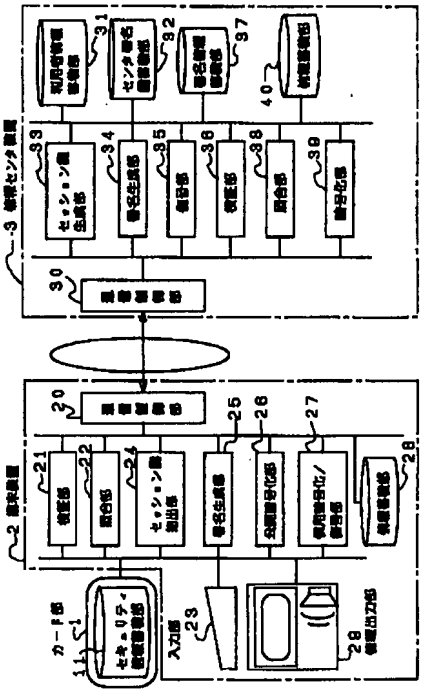
最終頁に続く

(54)【発明の名称】　ディジタル情報通信システム及びその方法

(57)【要約】

【目的】　情報の不正使用を防止できるディジタル情報通信システム及びその方法、並びに情報の利用端末が限定されないディジタル情報通信システム及びその方法を提供する。

【構成】　利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積部１１を有するカード部１を設け、端末装置２から情報センタ装置３に情報を要求する際に、カード部１と端末装置２とを接続し、カード部１に蓄積されている利用者識別番号を端末装置２から情報センタ装置３に送信する。さらに、情報センタ装置３から受信した情報本体をカード秘密鍵を用いて暗号化し端末装置２内に蓄積し、この情報本体を利用する際には、カード秘密鍵によって情報本体を復号する。これにより、端末装置２に依存することなく情報を利用することができる。



【特許請求の範囲】
【請求項１】　音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信システムにおいて、
利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設けると共に、
前記端末装置は、前記カード部を接続するインタフェース手段と、
前記情報センタ装置との間での通信を制御する通信制御手段と、
前記情報センタ装置から受信したディジタル署名情報を前記センタ検証鍵を用いて検証する検証手段と、
前記カード部に蓄積された利用者識別番号と、前記情報センタ装置から受信した利用者識別番号との照合を行なう照合手段と、
パスワードを入力する入力手段と、
該パスワードを用いて前記情報センタ装置から受信したセッション鍵を抽出するセッション鍵抽出手段と、
公開鍵暗号方式により、前記セッション鍵に対して前記カード部に蓄積された利用者署名鍵を用いてディジタル署名を行う署名生成手段と、
公開鍵暗号方式により、前記署名生成手段により得られた署名情報を前記センタ検証鍵によって暗号化処理を行なう公開暗号化手段と、
慣用暗号方式により、前記情報センタ装置から受信した情報を前記カード部に蓄積されたカード秘密鍵によって暗号化／復号処理を行なう慣用暗号化／復号手段と、
前記情報センタ装置からの受信情報を読出して利用できる形式に出力する情報出力手段とを備え、
前記情報センタ装置は、前記端末装置との間での通信を制御する通信制御手段と、
複数の登録利用者に対応する前記利用者識別番号、パスワード、利用者検証鍵を蓄積する利用者情報蓄積手段と、
センタの署名鍵を蓄積するセンタ署名鍵蓄積手段と、
ディジタル情報本体を暗号化するセッション鍵を生成するセッション鍵生成手段と、
公開鍵暗号方式により、前記セッション鍵に対して前記センタ署名鍵によってディジタル署名を行なう署名生成手段と、
公開鍵暗号方式により、前記端末装置から受信した暗号化署名情報の復号処理を行なう復号手段と、
該復号手段によって得られたディジタル署名情報を前記利用者検証鍵を用いて検証する検証手段と、
前記ディジタル署名情報を蓄積する署名情報蓄積手段と、
前記端末装置から受信したセッション鍵と、前記セッション鍵生成手段によって生成したセッション鍵との照合を行なう照合手段と、
ディジタル情報本体を蓄積する情報蓄積手段と、
共通鍵暗号方式により、前記セッション鍵を用いて前記情報蓄積手段内の送信対象となるディジタル情報本体の暗号化処理を行う暗号化手段とを備えることを特徴とするディジタル情報通信システム。
【請求項２】　カード秘密鍵、センタ検証鍵は同一値で、利用者識別番号、利用者署名鍵が異なる値を有する複数のカード部を有することを特徴とする請求項１記載のディジタル情報通信システム。
【請求項３】　音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信方法であって、
利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設け、
前記端末装置では、前記カード部のセキュリティ情報蓄積手段より抽出した利用者識別番号を前記情報センタ装置に送信すると共にディジタル情報を要求し、
情報センタ装置では、複数の登録利用者に対応する利用者識別番号、パスワード、利用者検証鍵が蓄積されている利用者情報蓄積手段より前記端末装置から受信した利用者識別番号に対応するパスワードを抽出し、次いで、セッション鍵を生成して、前記利用者識別番号、パスワード及び該セッション鍵を秘密関数で変換した後、該変換結果をセンタ署名鍵蓄積手段より抽出した署名鍵で署名し、前記端末装置に送信し、
前記端末装置では、前記情報センタから受信した署名情報を、前記カード部のセキュリティ情報蓄積手段より抽出したセンタ検証鍵で検証して利用者識別番号を取り出し、前記送信した利用者識別番号と比較し、該比較結果が不一致の場合には前記情報センタ装置との回線を切断し、前記比較結果が一致の場合には前記受信情報を秘密関数で変換してセッション鍵を抽出し、該セッション鍵を利用者署名鍵で署名した後、該署名情報をセンタ検証鍵で暗号化して前記情報センタ装置に送信し、
情報センタ装置では、前記端末装置から受信した暗号化署名情報を復号し、署名情報を署名情報蓄積手段に蓄積した後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とを照合し、該照合結果が不一致の場合には前記端末装置との回線を切断し、前記照合結果が一致の場合には前記端末装置から要求のあった情報を前記セッション鍵で慣用暗号化を行なった後、前記端末装置に送信し、
端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵を、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗

号化して、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積した後、
端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードを、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号して、入力手段より入力したパスワードと照合し、該照合結果が不一致の場合は情報の利用を禁止し、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体を復号して情報出力手段より出力することを特徴とするディジタル情報通信方法。
【請求項４】　音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信方法であって、
利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設け、
前記情報センタ装置の利用者情報蓄積手段に、登録利用者の利用者識別番号、利用者検証鍵及び利用者検証鍵で暗号化されたパスワードを蓄積しておき、
前記端末装置では、前記カード部のセキュリティ情報蓄積手段より抽出した利用者識別番号を前記情報センタ装置に送信すると共にディジタル情報を要求し、
情報センタ装置では、前記利用者情報蓄積手段より前記端末装置から受信した利用者識別番号に対応する暗号化パスワードを抽出し、次いで、セッション鍵を生成して、利用者検証鍵で検証してから、前記利用者識別番号、暗号化パスワード及び暗号化セッション鍵をセンタ署名鍵蓄積手段より抽出した署名鍵で署名して端末装置に送信し、
端末装置では、前記情報センタ装置から受信した署名情報を、前記カード部のセキュリティ情報蓄積手段より抽出したセンタ検証鍵で検証して利用者識別番号を取り出し、さらに、暗号化パスワードをそれぞれ比較していずれか不一致の場合には前記情報センタ装置との回線を切断し、利用者識別番号、パスワードともに一致の場合には前記情報センタ装置から受信した暗号化セッション鍵を利用者署名鍵で署名した後、該署名情報をセンタ検証鍵で暗号化して前記情報センタ装置に送信し、
情報センタ装置では、前記端末装置から受信した暗号化署名情報を復号し、署名情報を署名情報蓄積手段に蓄積した後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とを照合し、該照合結果が不一致の場合には前記端末装置との回線を切断し、前記照合結果が一致の場合には前記端末装置から要求のあった情報を前記セッション鍵で慣用暗号化を行なった後、前記端末装置に送信し、
端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵を、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗号化して、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積した後、
端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードを、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号して、入力手段より入力したパスワードと照合し、該照合結果が不一致の場合は情報の利用を禁止し、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体を復号して情報出力手段より出力することを特徴とするディジタル情報通信方法。
【請求項５】　音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信方法であって、
利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設け、
端末装置では、前記カード部のセキュリティ情報蓄積手段より抽出した利用者識別番号を前記情報センタ装置に送信すると共にディジタル情報を要求し、
前記情報センタ装置では、乱数を生成して前記端末装置に送信し、
前記端末装置では、入力したパスワードを利用者署名鍵で署名し、さらに暗号化パスワード及び前記情報センタ装置から受信した乱数をセンタ検証鍵で検証して前記情報センタ装置に送信し、
前記情報センタ装置では、前記端末装置から受信した暗号化情報をセンタ署名鍵で署名し、さらに、暗号化パスワードを利用者検証鍵で検証して得られた乱数、パスワードを、前記送信した乱数と利用者情報蓄積手段内のパスワードとそれぞれ照合して、いずれかが不一致の場合は前記端末装置との回線を切断し、乱数、パスワードともに一致の場合はセッション鍵を生成し、該セッション鍵を利用者検証鍵で暗号化して前記端末装置に送信し、
前記端末装置では、前記情報センタ装置から受信した暗号化セッション鍵を利用者署名鍵で署名した後、該署名情報をセンタ検証鍵で暗号化して前記情報センタ装置に返送し、
情報センタ装置では、前記端末装置から受信した暗号化署名情報を復号し、署名情報を署名情報蓄積手段に蓄積した後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とを照合し、該照合結果が不一致の場合には前記端末装置との回線を切断し、前記照合結果が一致の場合には前記端末装置から要求のあった情報を前記セッション鍵で慣用暗号化を行なった後、前記端末装置に送信し、

端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵を、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗号化して、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積した後、
端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードを、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号して、入力手段より入力したパスワードと照合し、該照合結果が不一致の場合は情報の利用を禁止し、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体を復号して情報出力手段より出力することを特徴とするディジタル情報通信方法。
【請求項6】　音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信方法であって、
利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設け、
情報を受信した受信端末装置とは異なる端末装置で前記受信情報を利用する際、該利用端末装置から、前記情報を受信した情報端末装置に接続し、
該情報端末装置の情報蓄積手段から利用したい情報に対応する暗号化パスワードを利用端末装置で受信し、
情報センタ装置から情報を受信時に使用したカード部から抽出したカード秘密鍵で復号して、利用端末装置の入力手段により入力したパスワードと照合し、該照合結果が不一致の場合は情報利用を禁止し、一致の場合は前記情報端末装置より、利用したい情報に対応する暗号化セッション鍵を受信し、前記カード秘密鍵で復号してセッション鍵を得た後、前記情報端末装置より利用したい暗号化された情報本体を受信し、該情報本体を利用端末装置において前記セッション鍵により復号して情報出力手段より出力することを特徴とするディジタル情報通信方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、音楽、映像、プログラム等の暗号化されたディジタル著作物の情報を、通信回線を経由して受信して蓄積した後、情報を利用する際、利用者にとって使いやすく、情報提供者にとって著作権の保護を考慮したディジタル情報通信システムおよびその方法に関するものである。
【０００２】
【従来の技術】近年、音声・動画・静止画等のディジタル情報圧縮技術（例えば、ＭＰＥＧ=Moving Picture Image Coding Expert Group，ＫＰＥＧ=Joint Photographic Expert Groupなど）、及びＩＳＤＮを代表とする高速ディジタル通信技術の発達により音楽・映像・絵画・書籍等の著作物をディジタル情報に変換すると共に圧縮符号化し、通信回線を利用して送信することが実現可能となってきた。映像などのディジタル情報に比べてデータ量の少ないコンピュータソフトウェアでは、既にパソコン通信などを利用した配送サービスを実施している例がある。
【０００３】ＩＳＤＮ通信回線を利用してディジタル情報を送信することにより、従来の流通経路が簡略化されるため、経済的でかつ迅速に情報を全国配送できる利点を有する。
【０００４】
【発明が解決しようとする課題】しかしながら、通信利用により受信して蓄積した優良のディジタル情報を使用する場合、情報を受信・購入した正規利用者だけでなく、他の利用者の不正使用の可能性が高まり、著作権侵害により、著作権者、情報提供業者の利益を損ねる問題が生じる。また、正規利用者にとって、通常は、情報を受信した端末装置の設置場所にいなくては情報の利用が不可能となる欠点があった。
【０００５】本発明の目的は上記の問題点に鑑み、情報の不正使用を防止できるディジタル情報通信システム及びその方法、並びに情報の利用端末が限定されないディジタル情報通信システム及びその方法を提供することにある。
【０００６】
【課題を解決するための手段】本発明は上記の目的を達成するために、請求項１では、音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信システムにおいて、利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設けると共に、前記端末装置は、前記カード部を接続するインタフェース手段と、前記情報センタ装置との間での通信を制御する通信制御手段と、前記情報センタ装置から受信したディジタル署名情報を前記センタ検証鍵を用いて検証する検証手段と、前記カード部に蓄積された利用者識別番号と、前記情報センタ装置から受信した利用者識別番号との照合を行なう照合手段と、パスワードを入力する入力手段と、該パスワードを用いて前記情報センタ装置から受信したセッション鍵を抽出するセッション鍵抽出手段と、公開鍵暗号方式により、前記セッション鍵に対して前記カード部に蓄積された利用者署名鍵を用いてディジタル署名を行う署名生成手段と、公開鍵暗号方式により、前記署名生成手段により得られた署名情報を前記センタ検証鍵によって暗号化処理を行なう公開暗号化手段と、慣用暗号方式により、

前記情報センタ装置から受信した情報を前記カード部に蓄積されたカード秘密鍵によって暗号化／復号処理を行なう慣用暗号化／復号手段と、前記情報センタ装置からの受信情報を読出して利用できる形式に出力する情報出力手段とを備え、前記情報センタ装置は、前記端末装置との間での通信を制御する通信制御手段と、複数の登録利用者に対応する前記利用者識別番号、パスワード、利用者検証鍵を蓄積する利用者情報蓄積手段と、センタの署名鍵を蓄積するセンタ署名鍵蓄積手段と、ディジタル情報本体を暗号化するセッション鍵を生成するセッション鍵生成手段と、公開鍵暗号方式により、前記セッション鍵に対して前記センタ署名鍵によってディジタル署名を行なう署名生成手段と、公開鍵暗号方式により、前記端末装置から受信した暗号化署名情報の復号処理を行なう復号手段と、該復号手段によって得られたディジタル署名情報を前記利用者検証鍵を用いて検証する検証手段と、前記ディジタル署名情報を蓄積する署名情報蓄積手段と、前記端末装置から受信したセッション鍵と、前記セッション鍵生成手段によって生成したセッション鍵との照合を行なう照合手段と、ディジタル情報本体を蓄積する情報蓄積手段と、共通鍵暗号方式により、前記セッション鍵を用いて前記情報蓄積手段内の送信対象となるディジタル情報本体の暗号化処理を行う暗号化手段とを備えるディジタル情報通信システムを提案する。

【０００７】また、請求項２では、請求項１記載のディジタル情報通信システムにおいて、カード秘密鍵、センタ検証鍵は同一値で、利用者識別番号、利用者署名鍵が異なる値を有する複数のカード部を有するディジタル情報通信システムを提案する。

【０００８】また、請求項３では、音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信方法であって、利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設け、前記端末装置では、前記カード部のセキュリティ情報蓄積手段より抽出した利用者識別番号を前記情報センタ装置に送信すると共にディジタル情報を要求し、情報センタ装置では、複数の登録利用者に対応する利用者識別番号、パスワード、利用者検証鍵が蓄積されている利用者情報蓄積手段より前記端末装置から受信した利用者識別番号に対応するパスワードを抽出し、次いで、セッション鍵を生成して、前記利用者識別番号、パスワード及び該セッション鍵を秘密関数で変換した後、該変換結果をセンタ署名鍵蓄積手段より抽出した署名鍵で署名し、前記端末装置に送信し、前記端末装置では、前記情報センタから受信した署名情報を、前記カード部のセキュリティ情報蓄積手段より抽出したセンタ検証鍵で検証して利用者識別番号を取り出し、前記送信した利用者識別番号と比較し、該比較結果が不一致の場合には前記情報センタ装置との回線を切断し、前記比較結果が一致の場合には前記受信情報を秘密関数で変換してセッション鍵を抽出し、該セッション鍵を利用者署名鍵で署名した後、該署名情報をセンタ検証鍵で暗号化して前記情報センタ装置に送信し、情報センタ装置では、前記端末装置から受信した暗号化署名情報を復号し、署名情報を署名情報蓄積手段に蓄積した後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とを照合し、該照合結果が不一致の場合には前記端末装置との回線を切断し、前記照合結果が一致の場合には前記端末装置から要求のあった情報を前記セッション鍵で慣用暗号化を行なった後、前記端末装置に送信し、端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵を、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗号化して、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積した後、端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードを、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号して、入力手段より入力したパスワードと照合し、該照合結果が不一致の場合は情報の利用を禁止し、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体を復号して情報出力手段より出力するディジタル情報通信方法を提案する。

【０００９】また、請求項４では、音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信方法であって、利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設け、前記情報センタ装置の利用者情報蓄積手段に、登録利用者の利用者識別番号、利用者検証鍵及び利用者検証鍵で暗号化されたパスワードを蓄積しておき、前記端末装置では、前記カード部のセキュリティ情報蓄積手段より抽出した利用者識別番号を前記情報センタ装置に送信すると共にディジタル情報を要求し、情報センタ装置では、前記利用者情報蓄積手段より前記端末装置から受信した利用者識別番号に対応する暗号化パスワードを抽出し、次いで、セッション鍵を生成して、利用者検証鍵で検証してから、前記利用者識別番号、暗号化パスワード及び暗号化セッション鍵をセンタ署名鍵蓄積手段より抽出した署名鍵で署名して端末装置に送信し、端末装置では、前記情報センタ装置から受信した署名情報を、前記カード部のセキュリティ情報蓄積手段より抽出したセンタ検証鍵で検証して利用者識別番号を取り出し、さらに、暗号化パスワードをそれぞれ比較して

いずれか不一致の場合には前記情報センタ装置との回線を切断し、利用者識別番号、パスワードともに一致の場合には前記情報センタ装置から受信した暗号化セッション鍵を利用者署名鍵で署名した後、該署名情報をセンタ検証鍵で暗号化して前記情報センタ装置に送信し、情報センタ装置では、前記端末装置から受信した暗号化署名情報を復号し、署名情報を署名情報蓄積手段に蓄積した後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とを照合し、該照合結果が不一致の場合には前記端末装置との回線を切断し、前記照合結果が一致の場合には前記端末装置から要求のあった情報を前記セッション鍵で慣用暗号化を行なった後、前記端末装置に送信し、端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵を、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗号化して、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積した後、端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードを、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号して、入力手段より入力したパスワードと照合し、該照合結果が不一致の場合は情報の利用を禁止し、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体を復号して情報出力手段より出力するディジタル情報通信方法を提案する。

【００１０】また、請求項５では、音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信方法であって、利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設け、端末装置では、前記カード部のセキュリティ情報蓄積手段より抽出した利用者識別番号を前記情報センタ装置に送信すると共にディジタル情報を要求し、前記情報センタ装置では、乱数を生成して前記端末装置に送信し、前記端末装置では、入力したパスワードを利用者署名鍵で署名し、さらに暗号化パスワード及び前記情報センタ装置から受信した乱数をセンタ検証鍵で検証して前記情報センタ装置に送信し、前記情報センタ装置では、前記端末装置から受信した暗号化情報をセンタ署名鍵で署名し、さらに、暗号化パスワードを利用者検証鍵で検証して得られた乱数、パスワードを、前記送信した乱数と利用者情報蓄積手段内のパスワードとそれぞれ照合して、いずれかが不一致の場合は前記端末装置との回線を切断し、乱数、パスワードともに一致の場合はセッション鍵を生成し、該セッション鍵を利用者検証鍵で暗号化して前記端末装置に送信し、前記端末装置では、前記情報センタ装置から受信した暗号化セッション鍵を利用者署名鍵で署名した後、該署名情報をセンタ検証鍵で暗号化して前記情報センタ装置に返送し、情報センタ装置では、前記端末装置から受信した暗号化署名情報を復号し、署名情報を署名情報蓄積手段に蓄積した後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とを照合し、該照合結果が不一致の場合には前記端末装置との回線を切断し、前記照合結果が一致の場合には前記端末装置から要求のあった情報を前記セッション鍵で慣用暗号化を行なった後、前記端末装置に送信し、端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵を、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗号化して、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積した後、端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードを、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号して、入力手段より入力したパスワードと照合し、該照合結果が不一致の場合は情報の利用を禁止し、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体を復号して情報出力手段より出力するディジタル情報通信方法を提案する。

【００１１】また、請求項６では、音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、該受信情報を端末装置に蓄積した後、該受信情報を復号してから利用するディジタル情報通信方法であって、利用者識別番号、カード秘密鍵、利用者署名鍵および、センタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカード部を設け、情報を受信した受信端末装置とは異なる端末装置で前記受信情報を利用する際、該利用端末装置から、前記情報を受信した情報端末装置に接続し、該情報端末装置の情報蓄積手段から利用したい情報に対応する暗号化パスワードを利用端末装置で受信し、情報センタ装置から情報を受信時に使用したカード部から抽出したカード秘密鍵で復号して、利用端末装置の入力手段により入力したパスワードと照合し、該照合結果が不一致の場合は情報利用を禁止し、一致の場合は前記情報端末装置より、利用したい情報に対応する暗号化セッション鍵を受信し、前記カード秘密鍵で復号してセッション鍵を得た後、前記情報端末装置より利用したい暗号化された情報本体を受信し、該情報本体を利用端末装置において前記セッション鍵により復号して情報出力手段より出力するディジタル情報通信方法を提案する。

【００１２】

【作用】本発明の請求項１によれば、カード部のセキュリティ情報蓄積手段には、利用者識別番号、カード秘密鍵、利用者署名鍵、及びセンタ検証鍵が蓄積される。また、端末装置と情報センタ装置との間の情報の授受はそ

れぞれに設けられた通信制御手段によって行われ、前記端末装置から前記情報センタ装置に情報を要求する際には、インタフェース手段を介して前記端末装置と前記カード部とが接続され、前記カード部のセキュリティ情報蓄積手段に蓄積されている利用者識別番号が前記情報センタ装置に送信される。前記利用者識別番号を受信した情報センタ装置では、該利用者識別番号に対応するパスワードが利用者情報蓄積手段から検索されると共に、セッション鍵生成手段によりディジタル情報本体を暗号化するセッション鍵が生成された後、該セッション鍵、利用者識別番号及びパスワードに対して、センタ署名鍵蓄積手段に蓄積されているセンタ署名鍵を用いて署名生成手段によって署名され、前記端末装置に送信される。該署名情報を受信した端末装置では、検証手段によって前記カード部のセキュリティ情報蓄積手段に蓄積されているセンタ検証鍵を用いて前記署名情報が検証され、該署名情報から利用者識別番号が取り出される。次いで、照合手段によって、該識別番号と前記カード部に蓄積された利用者識別番号との照合が行なわれ、該照合の結果、これらの利用者識別番号が一致した場合に、セッション鍵抽出手段によって入力手段から入力されたパスワードを用いて、前記署名情報から前記セッション鍵が抽出される。この後、セッション鍵を受信した確認として、署名生成手段により、該セッション鍵に対して前記カード部に蓄積されている利用者署名鍵を用いて署名がなされると共に、公開暗号化手段によってセンタ検証鍵で暗号化され、前記情報センタ装置に送信される。該暗号化署名情報を受信した情報センタ装置では、復号手段によって該暗号化署名情報が復号され、署名情報蓄積手段に蓄積される。さらに、検証手段によって該署名情報は利用者情報蓄積手段に蓄積されている利用者検証鍵によって検証されると共に、照合手段によって、前記端末装置から受信したセッション鍵と、前記セッション鍵生成手段によって生成されたセッション鍵との照合が行なわれ、該照合の結果これらが一致した場合、前記端末装置から要求のあった情報本体が情報蓄積手段から取り出されて、暗号化手段により暗号化処理が行われた後、前記端末装置に送信される。要求した情報本体を受信した端末装置では、慣用暗号化／復号手段により入力されたパスワードと情報センタ装置から受信したセッション鍵が前記カード秘密鍵で暗号化されると共に、受信した暗号化ディジタル情報本体と共に蓄積され、該情報本体を利用する際には、情報出力手段によって前記情報本体が読み出され、利用できる形式に変換されて出力される。

【００１３】また、請求項２によれば、ディジタル情報通信システムには、カード秘密鍵及びセンタ検証鍵が同一値であり、利用者識別番号及び利用者署名鍵が異なる値を有する複数のカード部が設けられている。これにより、カード秘密鍵及びセンタ検証鍵が同一値であるカード部を所有する者が要求した情報は、同一値のカード秘密鍵及びセンタ検証鍵を有するカード部を所有する他の者でも使用可能となる。

【００１４】また、請求項３によれば、端末装置からカード部のセキュリティ情報蓄積手段より抽出した利用者識別番号が情報センタ装置に送信されると共にディジタル情報が要求され、該要求を受けた情報センタ装置では、複数の登録利用者に対応する利用者識別番号、パスワード、利用者検証鍵が蓄積されている利用者情報蓄積手段より前記端末装置から受信した利用者識別番号に対応するパスワードが抽出され、次いで、セッション鍵が生成されて、前記利用者識別番号、パスワード及び該セッション鍵が秘密関数で変換された後、該変換結果はセンタ署名鍵蓄積手段より抽出した署名鍵を用いて署名され、前記端末装置に送信される。該署名情報を受信した端末装置では、前記情報センタから受信した署名情報は、前記カード部のセキュリティ情報蓄積手段より抽出したセンタ検証鍵で検証されて利用者識別番号が取り出され、前記送信した利用者識別番号と比較され、該比較結果が不一致の場合には前記情報センタ装置との回線が切断され、前記比較結果が一致の場合には前記受信情報は秘密関数で変換されてセッション鍵が抽出され、該セッション鍵が利用者署名鍵で署名された後、該署名情報がセンタ検証鍵で暗号化されて前記情報センタ装置に送信される。該暗号化署名情報受信した情報センタ装置では、前記端末装置から受信した暗号化署名情報が復号され、該署名情報が署名情報蓄積手段に蓄積された後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とが照合され、該照合結果が不一致の場合には前記端末装置との回線が切断され、前記照合結果が一致の場合には前記端末装置から要求のあった情報が前記セッション鍵で慣用暗号化された後、前記端末装置に送信される。この後、端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵が、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗号化されて、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積され、端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードが、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号されて、入力手段より入力したパスワードと照合され、該照合結果が不一致の場合は情報の利用が禁止され、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体が復号されて情報出力手段より出力される。

【００１５】また、請求項４によれば、情報センタ装置の利用者情報蓄積手段には、登録利用者の利用者識別番号、利用者検証鍵及び利用者検証鍵で暗号化されたパスワードが蓄積され、端末装置では、前記カード部のセキュリティ情報蓄積手段より抽出した利用者識別番号が前

記情報センタ装置に送信されると共にディジタル情報が要求される。前記端末装置から情報の要求を受けた情報センタ装置では、前記利用者情報蓄積手段より前記端末装置から受信した利用者識別番号に対応する暗号化パスワードが抽出され、次いで、セッション鍵が生成され、利用者検証鍵で検証されてから、前記利用者識別番号、暗号化パスワード及び暗号化セッション鍵に対してセンタ署名鍵蓄積手段より抽出した署名鍵で署名されて前記端末装置に送信される。該署名情報を受信した端末装置では、前記情報センタ装置から受信した署名情報が、カード部セキュリティ情報蓄積手段より抽出したセンタ検証鍵で検証されて利用者識別番号が取り出され、さらに、暗号化パスワードがそれぞれ比較されていずれか不一致の場合には前記情報センタ装置との回線が切断され、利用者識別番号、パスワードともに一致の場合には前記情報センタ装置から受信した暗号化セッション鍵が利用者署名鍵で署名された後、該署名情報がセンタ検証鍵で暗号化されて前記情報センタ装置に送信される。該暗号化署名情報を受信した情報センタ装置では、前記端末装置から受信した暗号化署名情報が復号され、署名情報が署名情報蓄積手段に蓄積された後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とが照合され、該照合結果が不一致の場合には前記端末装置との回線が切断され、前記照合結果が一致の場合には前記端末装置から要求のあった情報が前記セッション鍵で慣用暗号化された後、前記端末装置に送信される。この後、前記端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵が、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗号化されて、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積され、端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードが、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号されて、入力手段より入力したパスワードと照合され、該照合結果が不一致の場合は情報の利用が禁止され、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体が復号されて情報出力手段より出力される。

【００１６】また、請求項５によれば、情報要求の際には、端末装置では、カード部のセキュリティ情報蓄積手段より抽出した利用者識別番号が情報センタ装置に送信されると共にディジタル情報が要求され、該要求を受けた情報センタ装置では、乱数が生成されて前記端末装置に送信される。該乱数を受信した端末装置では、入力したパスワードが利用者署名鍵で署名され、さらに暗号化パスワード及び前記情報センタ装置から受信した乱数がセンタ検証鍵で検証されて前記情報センタ装置に送信される。この後、前記情報センタ装置では、前記端末装置から受信した暗号化情報がセンタ署名鍵で署名され、さらに、暗号化パスワードを利用者検証鍵で検証して得られた乱数及びパスワードが、前記送信した乱数と利用者情報蓄積手段内のパスワードとそれぞれ照合されて、いずれかが不一致の場合は前記端末装置との回線が切断され、乱数及びパスワード共に一致の場合はセッション鍵が生成され、該セッション鍵が利用者検証鍵で暗号化されて前記端末装置に送信される。次いで、前記端末装置では、前記情報センタ装置から受信した暗号化セッション鍵が利用者署名鍵で署名された後、該署名情報がセンタ検証鍵で暗号化されて前記情報センタ装置に返送される。さらに、情報センタ装置では、前記端末装置から受信した暗号化署名情報が復号され、署名情報が署名情報蓄積手段に蓄積された後、該署名情報を利用者検証鍵により検証して抽出したセッション鍵と前記生成したセッション鍵とが照合され、該照合結果が不一致の場合には前記端末装置との回線が切断され、前記照合結果が一致の場合には前記端末装置から要求のあった情報が前記セッション鍵で慣用暗号化された後、前記端末装置に送信される。この後、端末装置では、前記入力したパスワードと前記情報センタ装置から受信したセッション鍵が、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で暗号化されて、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積され、端末装置で情報を利用する際には、前記情報蓄積手段内の利用したい情報に対応する前記暗号化パスワードが、前記カード部のセキュリティ情報蓄積手段より抽出したカード秘密鍵で復号されて、入力手段より入力したパスワードと照合され、該照合結果が不一致の場合は情報の利用が禁止され、一致の場合は暗号化セッション鍵を前記カード秘密鍵で復号して得られたセッション鍵により暗号化された情報本体が復号されて情報出力手段より出力される。

【００１７】また、請求項６によれば、情報を受信した受信端末装置とは異なる端末装置で前記受信情報を利用する際には、該利用端末装置が前記情報を受信した情報端末装置に接続され、該情報端末装置の情報蓄積手段から利用したい情報に対応する暗号化パスワードが利用端末装置で受信され、情報センタ装置からの情報受信時に使用したカード部から抽出したカード秘密鍵で復号され、該復号されたパスワードと利用端末装置の入力手段により入力されたパスワードとが照合され、該照合結果が不一致の場合は情報利用が禁止される。また、照合結果が一致の場合は前記情報端末装置から前記利用端末装置に、利用したい情報に対応する暗号化セッション鍵が受信され、前記カード秘密鍵により復号されてセッション鍵を得た後、前記情報端末装置より利用したい暗号化された情報本体が受信され、該情報本体が利用端末装置において前記セッション鍵により復号されて情報出力手段より出力される。

【００１８】

【実施例】以下、図面に基づいて本発明の一実施例を説明する。図１は、本発明の第１の実施例を示す構成図である。図において、１はカード部で、利用者識別番号、カード秘密鍵、利用者署名鍵およびセンタ検証鍵を蓄積するセキュリティ情報蓄積部１１を備えており、例えば磁気カード、ＩＣカード、光記憶媒体からなるカード等を用いることが可能である。

【００１９】２は端末装置で、後述する情報センタ装置との間での通信を制御する通信制御部２０、情報センタ装置からのディジタル署名情報を検証する検証部２１、情報内容の照合を行なう照合部２２、パスワードを入力する入力部２３、情報センタ装置から受信したセッション鍵を抽出するセッション鍵抽出部２４、公開鍵暗号方式によりディジタル署名を行なう署名生成部２５、公開鍵暗号方式により暗号化処理を行なう公開暗号化部２６、慣用暗号方式により暗号化／復号処理を行う慣用暗号化／復号部２７、受信情報を蓄積する情報蓄積部２８、受信情報を読み出して利用できる形式に出する情報出力部２９を備えている。

【００２０】３は情報センタ装置で、端末装置２との間での通信を制御する通信制御部３０、複数の登録利用者に対応する前記利用者識別番号、パスワード、利用者検証鍵を蓄積する利用者情報蓄積部３１、センタの署名鍵を蓄積するセンタ署名鍵蓄積部３２、ディジタル情報本体を暗号化するセッション鍵を生成するセッション鍵生成部３３、公開暗号方式によりディジタル署名を行う署名生成部３４、公開鍵暗号方式により復号処理を行なう復号部３５、端末装置２からのディジタル署名情報を検証する検証部３６、前記ディジタル署名情報を蓄積する署名情報蓄積部３７、情報内容の照合を行なう照合部３８、共通鍵暗号方式により暗号化処理を行う暗号化部３９、ディジタル情報本体を蓄積する情報蓄積部４０を備えている。

【００２１】次に、前述の構成よりなる第１の実施例のディジタル情報通信システムにおける情報の受信、蓄積までの動作手順を図２に示すフローチャートに基づいて説明する。まず、情報を利用したい利用者のカード部１を端末装置２に接続する。接続方法は、カード部１を端末装置２のカード挿入用スロットに装入するか、有線ケーブルまたは赤外線、電波などの無線での接続などカード部１及び端末装置２の物理的構成・機能により様々に対応可能である。

【００２２】次いで、通信回線を介して端末装置２を情報センタ装置３に接続して、カード部１のセキュリティ情報蓄積部１１より抽出した利用者識別番号ＵＩＤｉを送信してディジタル情報内容を要求する（ＳＡ１）。図３に、カード部１のセキュリティ情報蓄積部１１の情報内容を示す。カード部１のセキュリティ情報蓄積部１１には、利用者識別番号ＵＩＤｉ、カード秘密鍵Ｋｉ、利用者署名鍵Ｄｉ、センタ検証鍵Ｃｐが蓄積されている。

【００２３】情報センタ装置３では、利用者情報蓄積部３１より、端末装置２から受信した前記利用者識別番号ＵＩＤｉに対応するパスワードＰＷｉを検索する（ＳＡ２）。図４に、利用者情報蓄積部３１の情報内容を示す。利用者情報蓄積部３１には、利用者識別番号ＵＩＤｉ、並びにこれに対応してパスワードＰＷｉ及び利用者検証鍵Ｅｉが蓄積されている。

【００２４】次いで、情報センタ装置３のセッション鍵生成部３３で、情報本体の暗号化用セッション鍵Session を生成する（ＳＡ３）。セッション鍵Session の生成方法は、乱数発生による生成など種々の方法があり、いずれの方法を用いることも可能である。この後、生成したセッション鍵Session 及び、前記検索した利用者識別番号ＵＩＤｉ、パスワードＰＷｉを特定の秘密関数で変換した（ＳＡ４）後、署名生成部３４において、この変換結果をセンタ署名鍵蓄積部３２により抽出した署名鍵Ｃｓで署名し（ＳＡ５）、端末装置２に送信する（ＳＡ６）。図５にセンタ署名鍵蓄積部３２の情報内容を示す。ここで、秘密関数は、端末装置２及び情報センタ装置３のみが知っている関数で、利用者には知らされていない関数である。例えば、秘密関数ｆは次の(1) 式によって表される。

【数１】

$$\text{秘密関数 } f(UIDi, PWi, Session) = UIDi \parallel PWi \oplus Session \quad \cdots(1)$$

‖はビット結合を表し、⊕は排他的論理和を表す。

また、ここで、署名とは、次の(2) 式に示すように、公開鍵暗号方式により情報センタ装置３の秘密鍵（署名鍵）Ｃｓで復号することを言う。

【００２５】

【数２】

$$Cs(UIDi \parallel PWi \oplus Session) \quad \cdots(2)$$

端末装置２では、検証部２１で、前記受信した署名情報を、カード部１のセキュリティ情報蓄積部１１より抽出したセンタ検証鍵Ｃｐで検証して利用者識別番号を取り出す（ＳＡ７）。ここで、検証とは、次の(3) 式に示すように、公開鍵暗号方式による情報センタ装置３の公開鍵（検証鍵）Ｃｐで暗号化することを言う。

【００２６】

【数３】

$$Cp(Cs(UIDi \parallel PWi \parallel Session)) = UIDi \parallel PWi \oplus Session \quad \cdots(3)$$

この後、照合部２２によって、前記取り出された利用者識別番号と、端末装置２から前記送信した利用者識別番号とを比較し（ＳＡ８）、この比較結果が不一致の場合には、情報センタ装置３との回線を切断する（ＳＡ

9）。また、前記ＳＡ８の比較結果が一致の場合には、セッション鍵抽出部２４により、前記受信情報から情報センタ装置３で使用したと同様の秘密関数で逆変換してセッション鍵を抽出する（ＳＡ１０）。

【００２７】前述した秘密関数の例では、次の(4) 式が成り立つため、

【数４】

$$PWi \oplus (PWi \oplus Session) - Session \quad \cdots(4)$$

入力部２３からパスワードを入力して、該パスワードと検証部２１の出力結果の排他的論理和を求めることにより、セッション鍵が得られる。

【００２８】次に、端末装置２は、セッション鍵を受信した確認として、次の(5) 式に示すように、署名生成部２５によって、受信したセッション鍵Session をカード部１のセキュリティ情報蓄積部１１より抽出した利用者署名鍵Ｄｉで署名すると共に（ＳＡ１１）、公開暗号化部２６によって、該署名情報をセンタ検証鍵Ｃｐで暗号化して（ＳＡ１２）、情報センタ装置３に送信する（ＳＡ１３）。

【００２９】

【数５】

$$Cp(Di(Session)) \quad \cdots(5)$$

この後、情報センタ装置３では、復号部３５により、次の(6) 式に示すように、前記受信した暗号化署名情報をセンタ署名鍵Ｃｓを用いて復号し（ＳＡ１４）、復号した署名情報を署名情報蓄積部３７に蓄積する（ＳＡ１５）。

【００３０】

【数６】

$$Cs(Cp(Di(Session))) = Di(Session) = \text{署名情報} \quad \cdots(6)$$

次に、情報センタ装置３は、検証部３６によって、この署名情報を利用者情報蓄積部３１内の利用者検証鍵Ｅｉにより検証すると共に（ＳＡ１６）、照合部３８により、抽出したセッション鍵と前記生成したセッション鍵とを照合し（ＳＡ１７）、この照合結果が不一致の場合には端末装置２との回線を切断し（ＳＡ１８）、一致の場合には端末装置２から要求のあった情報を情報蓄積部４０より取り出して、暗号化部３９により、次の(7) 式に示すように前記セッション鍵Session を用いて慣用暗号化を行ない（ＳＡ１９）、端末装置２に送信する（ＳＡ２０）。

【００３１】

【数７】

$$Session(\text{情報本体}) \quad \cdots(7)$$

端末装置２では、慣用暗号化／復号部２７によって、前記入力したパスワードＰＷｉと前記受信したセッション鍵Session を、カード部１のセキュリティ情報蓄積部１１より抽出したカード秘密鍵Ｋｉを用いて暗号化し（ＳＡ２１）、前記受信した暗号化ディジタル情報と共に情報蓄積部２８に蓄積する（ＳＡ２２）。情報蓄積部２８には図６に示すように、カード秘密鍵Ｋｉを用いて暗号化されたパスワードＰＷｉ及びセッション鍵Session 、並びにセッション鍵Session を用いて暗号化された情報本体が蓄積されている。

【００３２】なお、図２に示す端末装置２における利用者識別番号照合、情報センタ装置３におけるセッション鍵照合での不一致の場合、即回線を切断するのではなく、指定回数の再入力、再送信を繰り返した後、回線を切断するようにしてもよい。

【００３３】次に、第１の実施例のディジタル情報通信システムにおいて、受信した情報を端末装置２で利用する場合の手順を図７に示すフローチャートに基づいて説明する。

【００３４】端末装置２において情報センタ装置３から受信した情報を利用する際には、端末装置２の情報蓄積部２８に蓄積されている情報の中の利用したい情報に対応する前記暗号化パスワードＰＷｉを抽出すると共に（ＳＢ１）、慣用暗号化／復号部２７によって、カード部１のセキュリティ情報蓄積部１１より抽出したカード秘密鍵Ｋｉを用いて前記抽出した暗号化パスワードＰＷｉを復号する（ＳＢ２）。この後、照合部２２によって、複合したパスワードＰＷｉと入力部２３から入力したパスワードとを照合し（ＳＢ３）、この照合結果が不一致の場合には情報の利用を禁止する（ＳＢ４）。また、照合結果が一致の場合には、慣用暗号化／復号部２７によって、前記カード秘密鍵Ｋｉを用いて暗号化セッション鍵を復号すると共に（ＳＢ５）、これにより得られたセッション鍵を用いて暗号化された情報本体を慣用暗号化／復号部２７によって復号し（ＳＢ６）、複合した情報本体を情報出力部２９より出力する（ＳＢ７）。

【００３５】以上の手順では、端末装置２が情報センタ装置３から情報を受信する際、パスワードの照合は陽には行なわず、利用者識別番号の照合を端末装置２で行ない、セッション鍵の照合を情報センタ装置３で行なうことにより、結果的にパスワード照合を暗に実施して利用者の認証を行なっている。

【００３６】次に、情報センタ装置３から端末装置２に情報を受信する際の第２の実施例の動作手順を図８のフローチャートに基づいて説明する。ここで、第２の実施例は、パスワードを端末装置２側で照合する方法である。

【００３７】この際、情報センタ装置３の利用者情報蓄積部３１には、図９に示す通り登録利用者の利用者識別番号ＵＩＤｉ、利用者検証鍵で暗号化されたパスワードＥｉ（ＰＥｉ）及び利用者検証鍵Ｅｉを蓄積しておく。

【００３８】まず、端末装置２では、通信制御部２０を介して情報センタ装置３に接続し、カード部１内のセキュリティ情報蓄積部１１より抽出した利用者識別番号Ｕ

ＩＤｉを情報センタ装置３に送信してディジタル情報を要求する（ＳＣ１）。

【００３９】情報センタ装置３では、利用者情報蓄積部３１より前記受信した利用者識別番号ＵＩＤｉに対応する暗号化パスワードＥｉ（ＰＷｉ）を検索する（ＳＣ２）。次いで、セッション鍵生成部３３によりセッション鍵を生成した後（ＳＣ３）、検証部３６によって利用者検証鍵Ｅｉを用いてセッション鍵を検証してから（ＳＣ４）、署名生成部３４において、次の(8) 式に示すように、前記利用者識別番号、暗号化パスワード及び暗号化セッショ鍵に対して、センタ署名鍵蓄積部３２から抽出した署名鍵Ｃｓを用いて署名し（ＳＣ５）、端末装置２に送信する（ＳＣ６）。

【数８】

$$Cs(UIDi \| Ei(PWi) \| Ei(Session)) \quad \cdots(8)$$

この後、端末装置２では、次の(9) 式に示すように、前記受信した署名情報を、検証部２１で、カード部１内のセキュリティ情報蓄積部１１より抽出したセンタ検証鍵Ｃｐにより検証して利用者識別番号を取り出し（ＳＣ７）、さらに署名生成部２６で、暗号化パスワードを利用者署名鍵Ｄｉにより署名する（ＳＣ８）。

【００４０】

【数９】

$$Cp(UIDi \| Ei(PWi) \| Ei(Session)) = UIDi \| Ei(PWi) \| Ei(Session) \quad \cdots(9)$$

次に、端末装置２は前記送信した利用者識別番号と入力したパスワードをそれぞれ比較し（ＳＣ９）、この比較の結果、いずれかが不一致の場合には情報センタ装置３との回線を切断する（ＳＣ１０）。また、利用者識別番号及びパスワードともに一致の場合には、前記受信した暗号化セッション鍵を利用者署名鍵で署名した後（ＳＣ１１）、次の(10) 式に示すように公開暗号化部２６により、該署名情報をセンタ検証鍵Ｃｐで暗号化して（ＳＣ１２）、情報センタ装置３に送信する（ＳＣ１３）。

【００４１】

【数１０】

$$Cp(Di(Session)) \quad \cdots(10)$$

なお、これ以降のＳＣ１４～ＳＣ２２の処理（情報センタ装置３でもセッション鍵照合、情報本体配送、端末装置への蓄積手順）は、先に説明した第１の実施例におけるＳＡ１４～ＳＡ２２の処理手順と同一であるので、その説明を省略する。

【００４２】本第２の実施例の方式では、情報センタ装置３でパスワードそのものを蓄積しておかなくても良く、暗号化パスワードのみであるため情報センタ装置３のセキュリティ性が非常に高くなる。

【００４３】次に、情報センタ装置３から端末装置２に情報を受信する際の第３の実施例の動作手順を図１０のフローチャートに基づいて説明する。第３の実施例は、情報センタ装置３に各端末装置２のパスワードを保有して情報センタ装置３側でパスワードを照合する方法である。ここで、利用者情報蓄積部３１の内容は図４の内容と同様である。

【００４４】端末装置２では、情報センタ装置３に接続して、カード部１内のセキュリティ情報蓄積部１１より抽出した利用者識別番号を送信してディジタル情報を要求する（ＳＤ１）。

【００４５】情報センタ装置３では、任意の乱数Ｒを生成して（ＳＤ２）、端末装置２に送信する（ＳＤ３）。情報センタ装置３から乱数Ｒを受信した端末装置２では、入力部２３より入力したパスワードを署名生成部２５において利用者署名鍵Ｄｉにより署名し（ＳＤ４）、さらに公開暗号化部２６において、次の(11)式に示すように暗号化パスワード及び前記受信した乱数Ｒをセンタ検証鍵Ｃｐを用いて検証し（ＳＤ５）、情報センタ装置３に送信する（ＳＤ６）。

【００４６】

【数１１】

$$Cp(Di(PWi) \| R) \quad \cdots(11)$$

この後、情報センタ装置３では、署名生成部３４によって、前記受信した暗号化情報に対してセンタ署名鍵Ｃｓを用いて署名し（ＳＤ７）、さらに、暗号化パスワードを利用者検証鍵Ｅｉで検証する（ＳＤ８）。次に、照合部３８により、得られた乱数及びパスワードを、前記送信した乱数と利用者情報蓄積部３１内のパスワードとそれぞれ照合し（ＳＤ９）、この照合の結果、いずれかが不一致の場合には端末装置２と情報センタ装置３との回線を切断し（ＳＤ１０）、乱数及びパスワード共に一致の場合には、セッション鍵生成部３３においてセッション鍵を生成し（ＳＤ１１）、検証部３６で、利用者検証鍵Ｅｉを用いて検証し（ＳＤ１２）、端末装置２に送信する（ＳＤ１３）。

【００４７】この後、端末装置２では、次の(12)式に示すように、署名生成部２５において前記受信した暗号化セッション鍵を利用者署名鍵Ｄｉで署名した後（ＳＤ１４）、公開暗号化部２６で、該署名情報をセンタ検証鍵で暗号化して（ＳＤ１５）、情報センタ装置３に送信する（ＳＤ１６）。

【００４８】

【数１２】

$$Cp(Di(Session)) \quad \cdots(12)$$

なお、これ以降のＳＤ１７～ＳＤ２５の処理（情報センタ装置でセッション鍵照合及び情報本体配送を行い、端

末装置において受信情報を蓄積する手順）は、先に説明した第１の実施例におけるＳＡ１４～ＳＡ２２の処理手順と同一であるので、その説明を省略する。

【００４９】以上、第１乃至第３の実施例により、情報を受信した正規利用者のみがカード部１を用いて情報センタ装置３に蓄積されている情報を利用するディジタル情報通信システムを提供でき、情報の著作権保有者の保護が可能となる。

【００５０】次に、本発明の第４の実施例を図１１に基づいて説明する。第４の実施例は、情報を受信した受信端末装置とは異なる別対地にある端末装置から前記受信情報を利用する方法を示す。

【００５１】図１１において、端末装置Ａは、図１における情報センタ装置３からディジタル情報を受信して情報蓄積部２８に蓄積した装置を示し、端末装置Ｂは、端末装置Ａとは別対地にあり、端末装置Ａに蓄積されているディジタル情報を利用しようとする端末装置である。

【００５２】次に、前述の構成よりなる第４の実施例の動作手順を図１２に示すフローチャートに基づいて説明する。まず、ディジタル情報を利用したい利用者の所有するカード部１を端末装置Ｂに接続する（ＳＥ１）。次いで、端末装置Ｂを通信制御部２０を介して端末装置Ａに接続して（ＳＥ２）、端末装置Ａの情報蓄積部２８内の利用したい情報に対応する暗号化パスワードＰＷｉを抽出し（ＳＥ３）、端末装置Ｂに送信する（ＳＥ４）。この後、端末装置Ｂでは、慣用暗号化／復号部２７で、カード部１のセキュリティ情報蓄積部１１から抽出したカード秘密鍵Ｋｉで端末装置Ａから受信した暗号化パスワードを復号し（ＳＥ５）、照合部２２により、復号したパスワードと入力部２３から入力したパスワードとを照合し（ＳＥ６）、この照合の結果が不一致の場合には情報の利用を禁止して、端末装置Ａとの回線を切断する（ＳＥ７）。また、照合の結果、前記パスワードが一致する場合には、端末装置Ａでは暗号化セッション鍵および該セッション鍵で暗号化された情報本体を情報蓄積部２８より抽出して（ＳＥ８）、端末装置Ｂに送信する（ＳＥ９）。

【００５３】この後、端末装置Ｂでは、受信した暗号化セッション鍵をカード部１のセキュリティ情報蓄積部１１より抽出したカード秘密鍵Ｋｉで復号した後（ＳＥ１０）、該セッション鍵で暗号化された情報本体を復号して（ＳＥ１１）、この復号された情報本体を情報出力部２９より出力して利用する（ＳＥ１２）。

【００５４】なお、本第４の実施例は、他の端末装置Ｂから自分の端末装置Ａをアクセスして以前に端末装置Ａに受信したディジタル情報を利用する方法であるが、他の端末装置Ｂから直接情報センタ装置３にアクセスして新規ディジタル情報を受信して利用できることは言うまでもない。

【００５５】次に、本発明の第５の実施例として、複数のカード部１の集合を有する例を図１３に基づいて説明する。図１３に示す通り、カード秘密鍵Ｋｉ及びセンタ検証鍵Ｃｓは同一で、利用者識別番号ＵＩＤｉ並びに利用者署名鍵Ｄｉの異なる複数のカード部１を情報提供業者が発行する。例えば、家族、会社内セクションなど閉じたグループを対象として発行するカード部１である。これにより、本カード部１を保有しているグループ構成員のいずれかが受信したディジタル情報は、グループ構成員の誰でも自由にどこでも利用可能な環境を提供できる。その際、発行するカード数つまり、グループ構成員数によりディジタル情報受信の際の情報料金を変更すれば著作権者及び情報提供業者の利益を損ねることはない。

【００５６】

【発明の効果】以上説明したように本発明の請求項１記載のディジタル情報通信システムによれば、利用者の識別情報を記録したカード部を用いて、ディジタル情報を受信した後、端末装置に蓄積する際、暗号化された個人情報及び、情報復号鍵を合せて蓄積しておき、情報利用の際、前記利用者のカード部により個人情報を照合してから、情報を利用可能としているので、正規のディジタル情報利用者のみが該情報を利用でき、情報の不正使用を防止することができる。これにより、著作権侵害を防止できると共に、著作権者及び情報提供業者の利益を損ねることがない。また、利用者の所在、ディジタル情報の所在はどこにあっても利用できるシステムを提供でき、著作権の保護のため、また、利用者の利便性にとって大きな効果がある。さらに、端末装置は情報提供業者に依存せず、自由に製造して利用者に販売できる大きな利点がある。

【００５７】また、請求項２によれば、上記の効果に加えて、カード秘密鍵及びセンタ検証鍵は同一で、利用者識別番号並びに利用者署名鍵の異なる複数のカード部を情報提供業者が発行することにより、利用者側（利用人数の拡大）、情報提供業者側（情報料金の高額徴収）の両者にとって便利なシステムを提供できる大きな利点がある。

【００５８】また、請求項３乃至請求項５記載のディジタル情報通信方法によれば、利用者の識別情報を記録したカード部を用いて、ディジタル情報を受信した後、端末装置に蓄積する際、暗号化された個人情報及び、情報復号鍵を合せて蓄積しておき、情報利用の際、前記利用者のカード部により個人情報を照合してから、情報を利用可能としているので、正規のディジタル情報利用者のみが該情報を利用でき、情報の不正使用を防止することができる。これにより、著作権侵害を防止できると共に、著作権者及び情報提供業者の利益を損ねることがない。

【００５９】さらに、請求項４記載のディジタル情報通信方法によれば、上記の効果に加えて、情報センタ装置

側にパスワードを蓄積しておく必要がなく、情報センタ装置側のセキュリティ性を非常に高めることができる。

【００６０】また、請求項６記載のディジタル情報通信方法によれば、利用者の識別情報を記録したカード部を用いて、ディジタル情報を受信した後、端末装置に蓄積する際、暗号化された個人情報及び、情報復号鍵を合せて蓄積しておき、情報利用の際、前記利用者のカード部により個人情報を照合してから、情報を利用可能としているので、正規のディジタル情報利用者のみが該情報を利用でき、情報の不正使用を防止することができる。これにより、著作権侵害を防止できると共に、著作権者及び情報提供業者の利益を損ねることがない。さらに、情報の所在する端末装置とは別の端末装置から情報を取り出して利用できるので、著作権の保護のため、また、利用者の利便性にとって大きな効果を奏するものである。

【図面の簡単な説明】

【図１】本発明の第１の実施例のディジタル情報通信システムを示す構成図

【図２】第１の実施例における情報の受信、蓄積までの動作手順を示すフローチャート

【図３】第１の実施例におけるカード部内のセキュリティ情報蓄積部の情報内容を示す図

【図４】第１の実施例における利用者情報蓄積部の情報内容を示す図

【図５】第１の実施例におけるセンタ署名鍵蓄積部の情報内容を示す図

【図６】第１の実施例における情報蓄積部の情報内容を示す図

【図７】第１の実施例における端末装置で受信した情報を利用する場合の手順を示すフローチャート

【図８】本発明の第２の実施例における情報の受信、蓄積までの動作手順を示すフローチャート

【図９】第２の実施例において使用する利用者情報蓄積部の情報内容を示す図

【図１０】本発明の第３の実施例における情報の受信、蓄積までの動作手順を示すフローチャート

【図１１】本発明の第４の実施例示す構成図

【図１２】第４の実施例における情報利用手順を示すフローチャート

【図１３】本発明の第５の実施例における複数のカード部を説明する図

【符号の説明】

１…カード部、２…端末装置、３…情報センタ装置、１１…セキュリティ情報蓄積部、２０…通信制御部、２１…検証部、２２…照合部、２３…入力部、２４…セッション鍵抽出部、２５…署名生成部、２６…公開暗号化部、２７…慣用暗号化／復号部、２８…情報蓄積部、２９…情報出力部、３０…通信制御部、３１…利用者情報蓄積部、３２…センタ署名鍵蓄積部、３６…検証部、３７…署名情報蓄積部、３８…照合部、３９…暗号化部、４０…情報蓄積部。

【図３】

利用者識別番号	カード暗号鍵	利用者署名鍵	センタ検証鍵
UID1	K1	D1	Cp

【図４】

利用者識別番号	パスワード	利用者検証鍵
UID1	PW1	E1
：	：	：
UIDi	PWi	Ei
：	：	：

【図５】

センタ署名鍵
Cs

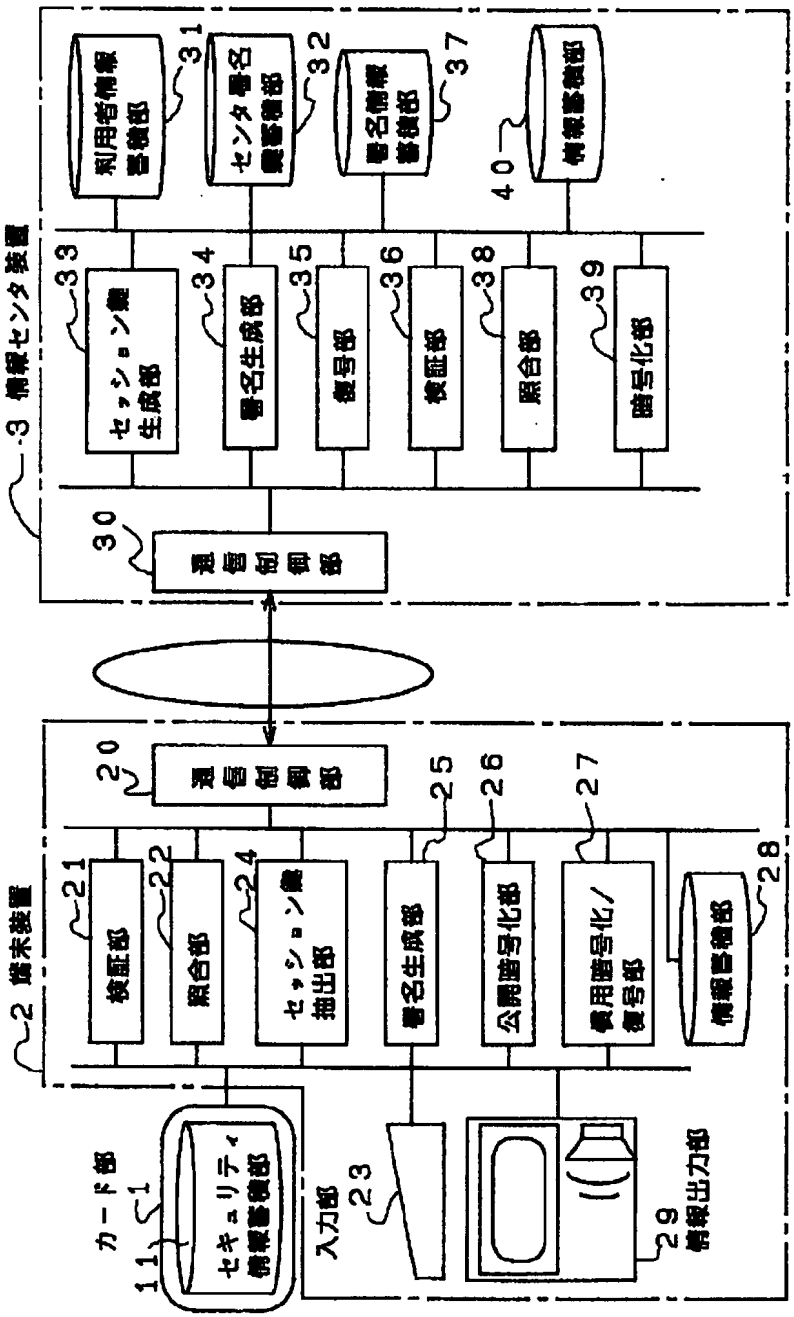
【図６】

K1(PW1)	Session（情報本体）
K1(Session)	

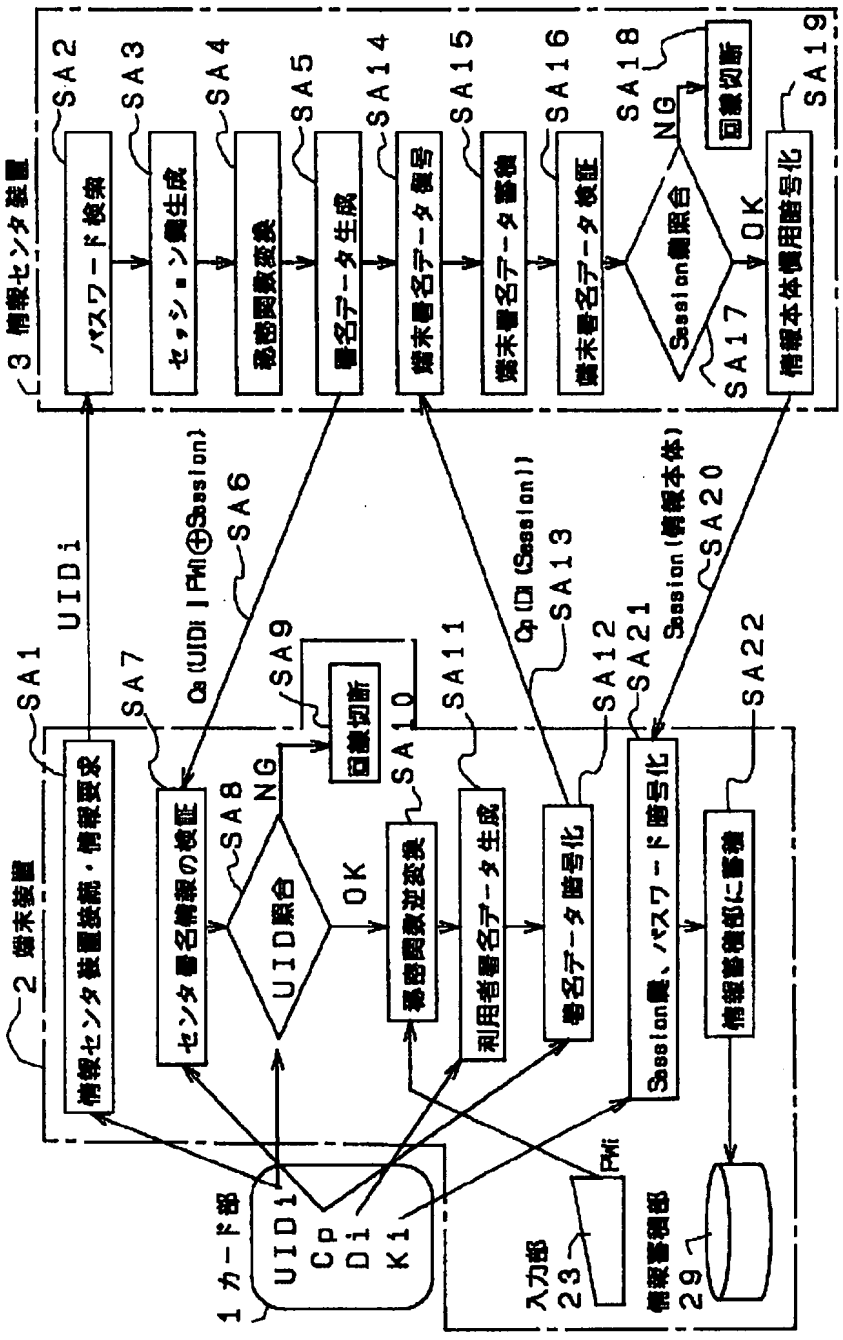
【図９】

利用者識別番号	暗号化パスワード	利用者検証鍵
UID1	E1(PW1)	E1
：	：	：
UIDi	Ei(PWi)	Ei
：	：	：

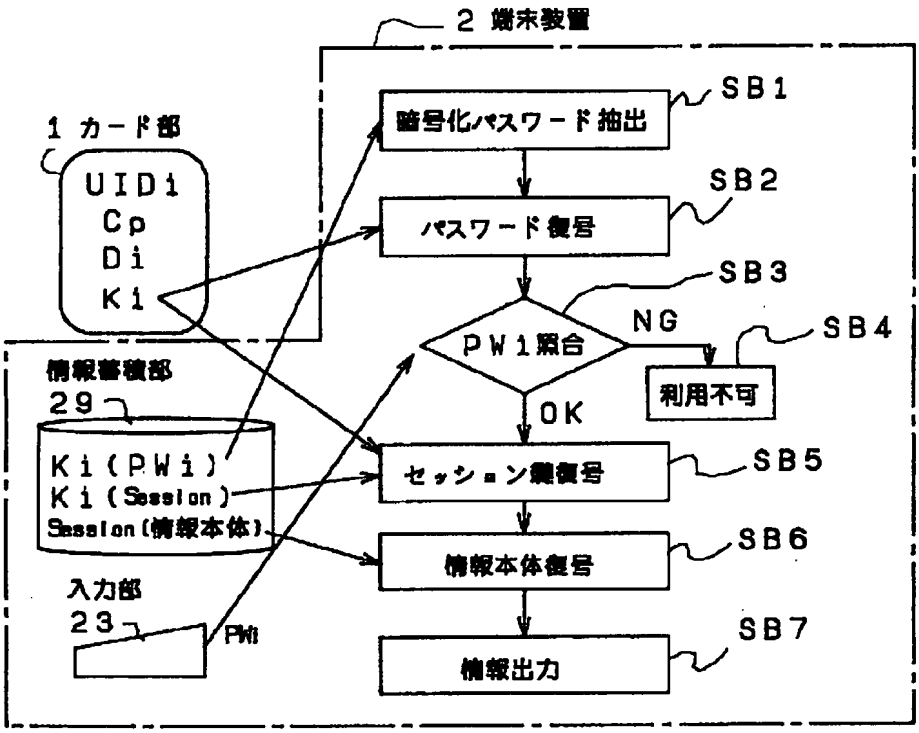
【図1】


3 情報センタ装置
利用者情報蓄積部
31
センタ署名鍵蓄積部
32
署名情報蓄積部
37
情報蓄積部
40
33
セッション鍵生成部
34
署名生成部
35
復号部
36
検証部
38
照合部
39
暗号化部
30
通信制御部
2 端末装置
通信制御部
20
検証部
21
照合部
22
セッション鍵抽出部
24
署名生成部
25
公開暗号化部
26
秘用暗号化／復号部
27
情報蓄積部
28
カード部
1
セキュリティ情報蓄積部
11
入力部
23
29
情報出力部

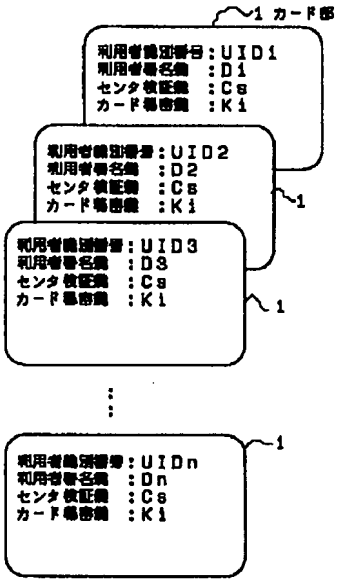
【図2】


3 情報センタ装置
SA2
パスワード検索
SA3
セッション鍵生成
SA4
秘密関数変換
SA5
署名データ生成
SA14
端末署名データ復号
SA15
端末署名データ蓄積
SA16
端末署名データ検証
SA18
Session鍵照合
NG
SA17
OK
回線切断
SA19
情報本体復用暗号化
UIDi
Cp(UIDi‖Pwi⊕Session)
SA6
Cp(Di‖Session)
SA13
Session(情報本体)
SA20
SA1
SA7
SA9
回線切断
SA11
SA12
SA21
SA22
2 端末装置
情報センタ装置接続・情報要求
センタ署名情報の検証
SA8
NG
UID照合
OK
秘密関数逆変換
SA10
利用者署名データ生成
署名データ暗号化
Session鍵、パスワード暗号化
情報蓄積部に蓄積
1 カード部
UIDi
Cp
Di
Ki
Pwi
入力部
23
情報蓄積部
29

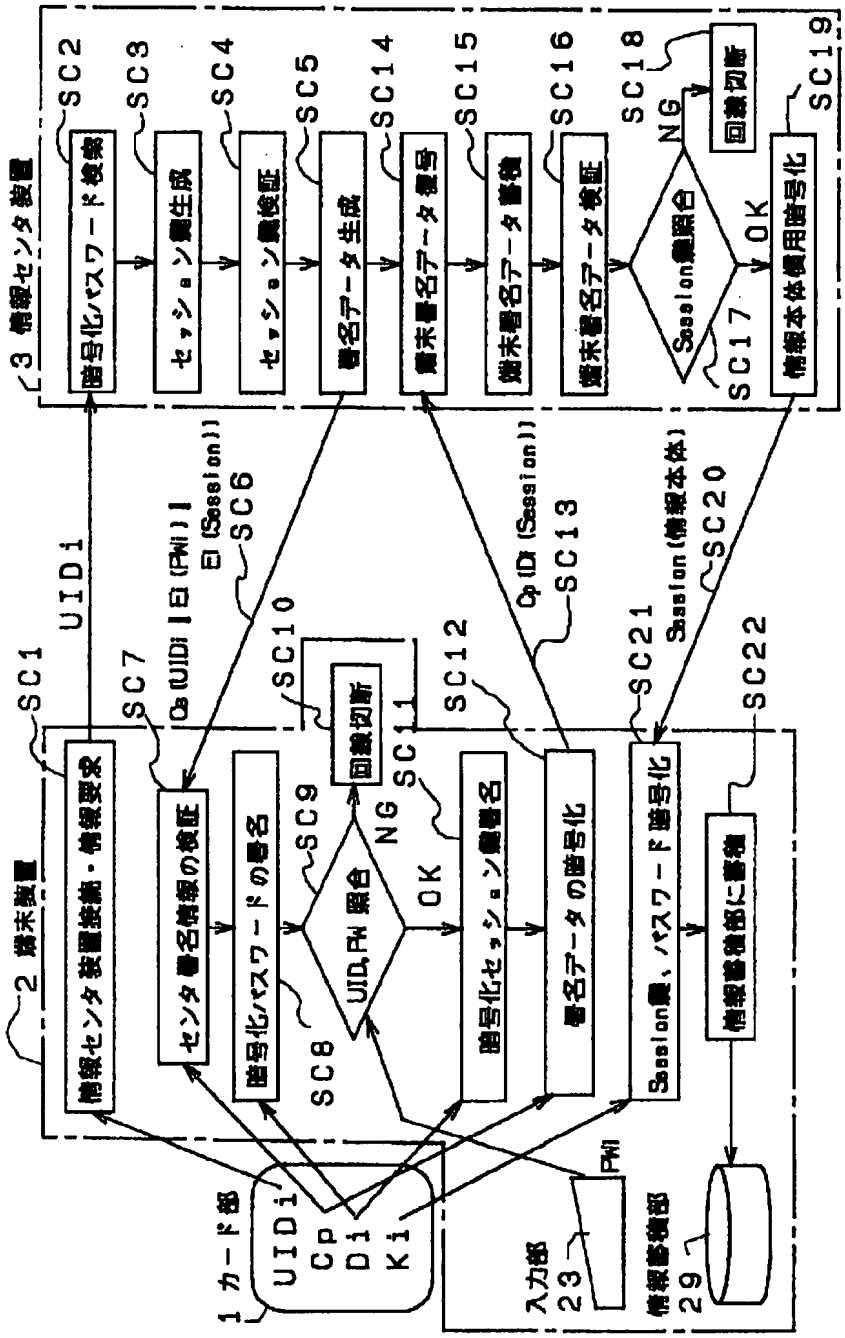
【図7】


2 端末装置
1 カード部
UIDi
Cp
Di
Ki
暗号化パスワード抽出
SB1
パスワード復号
SB2
PW1照合
SB3
NG
SB4
利用不可
OK
情報蓄積部
29
Ki(PWi)
Ki(Session)
Session(情報本体)
セッション鍵復号
SB5
情報本体復号
SB6
入力部
23
PWi
情報出力
SB7

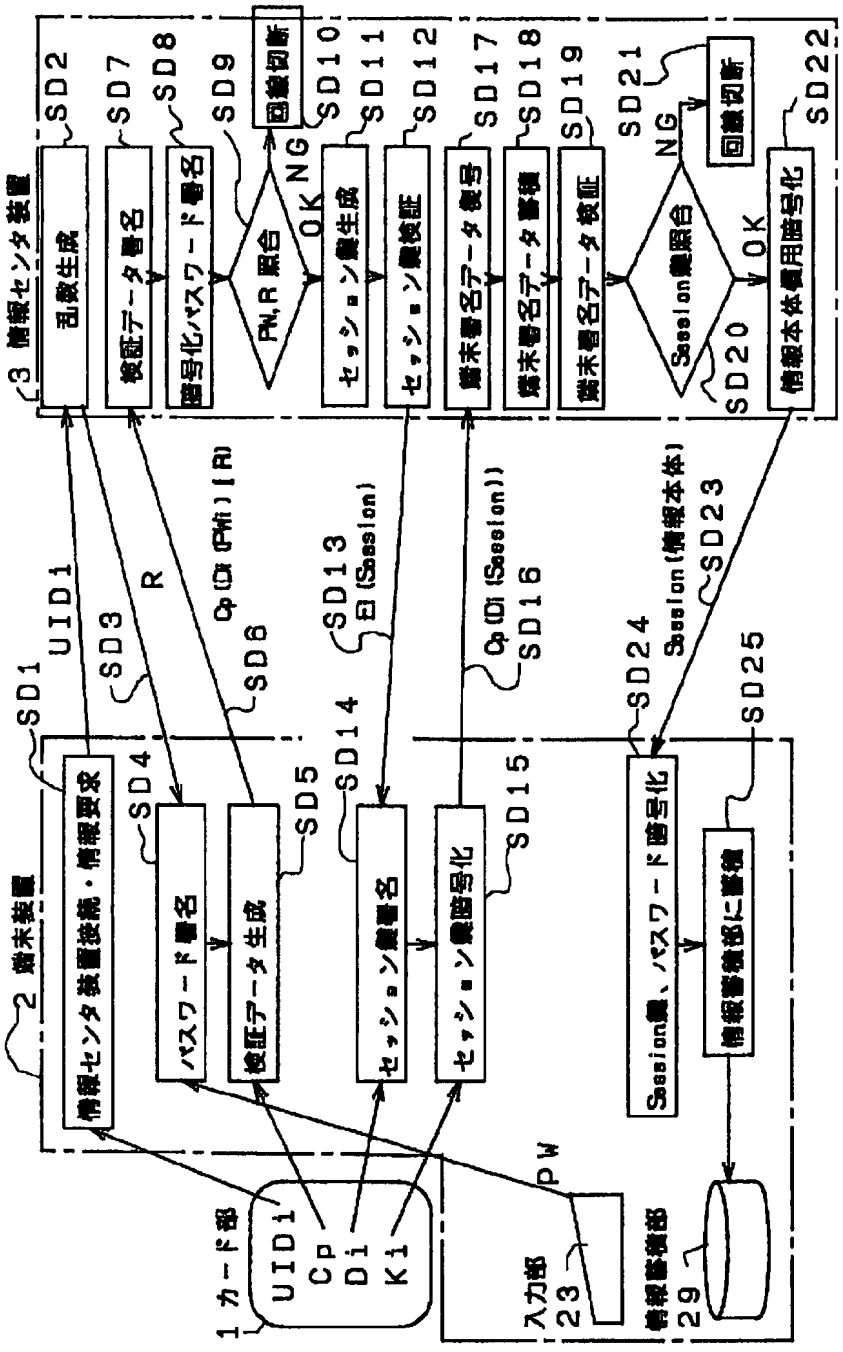
【図13】


1 カード部
利用者識別番号:UID1
利用者暗号鍵 :Di
センタ検証鍵 :Cs
カード暗号鍵 :Ki
利用者識別番号:UID2
利用者暗号鍵 :D2
センタ検証鍵 :Cs
カード暗号鍵 :Ki
1
利用者識別番号:UID3
利用者暗号鍵 :D3
センタ検証鍵 :Cs
カード暗号鍵 :Ki
1
利用者識別番号:UIDn
利用者暗号鍵 :Dn
センタ検証鍵 :Cs
カード暗号鍵 :Ki
1

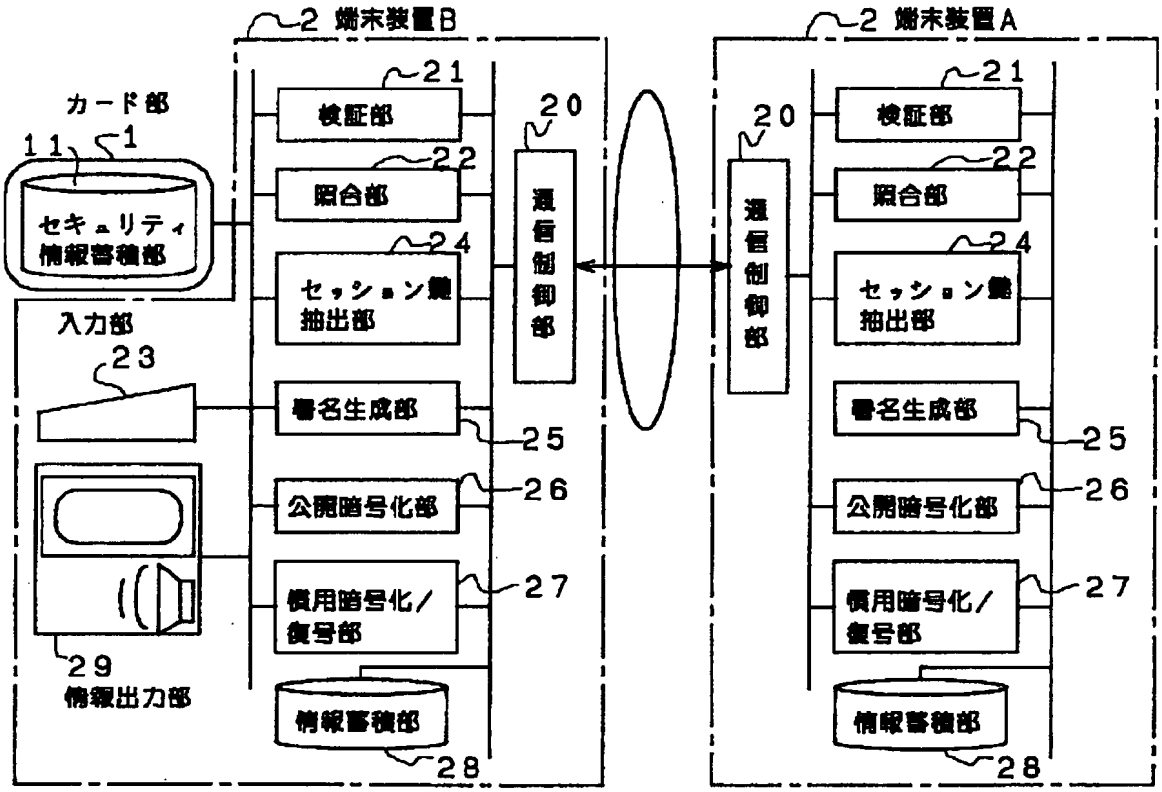
【図8】


3 情報センタ装置
2 端末装置
1 カード部
入力部
23
情報蓄積部
29
SC1
SC2
SC3
SC4
SC5
SC6
SC7
SC8
SC9
SC10
SC11
SC12
SC13
SC14
SC15
SC16
SC17
SC18
SC19
SC20
SC21
SC22
UIDi
Cp
Di
Ki
PWi
NG
OK
回線切断
暗号化パスワード検索
セッション鍵生成
セッション鍵検証
署名データ生成
端末署名データ蓄積
端末署名データ検証
Session鍵照合
情報本体鍵用暗号化
情報センタ装置接続・情報要求
センタ署名情報の検証
暗号化パスワードの署名
UID,PW 照合
暗号化セッション鍵署名
署名データの暗号化
Session鍵、パスワード暗号化
情報蓄積部に蓄積

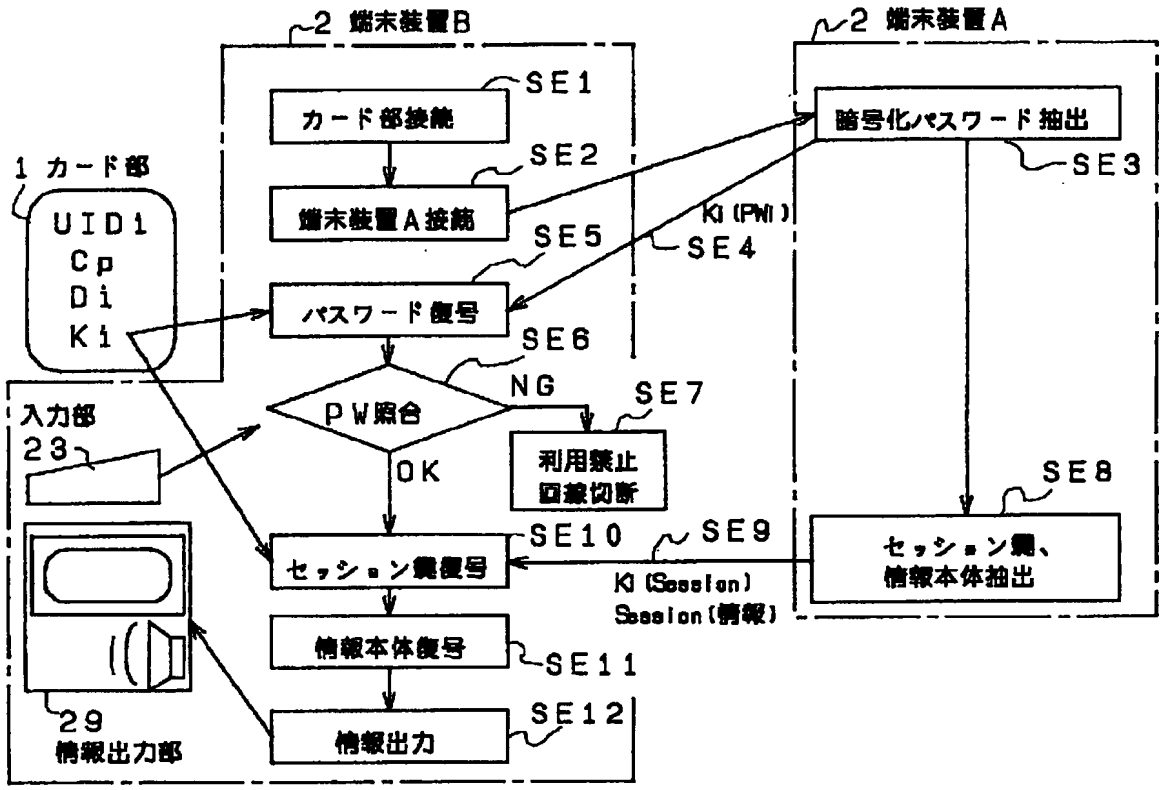
【図10】


3 情報センタ装置
乱数生成
検証データ署名
暗号化パスワード署名
P'W,R 照合
OK
NG
回線切断
セッション鍵生成
セッション鍵検証
端末署名データ復号
端末署名データ蓄積
端末署名データ検証
Session鍵照合
OK
NG
回線切断
情報本体鍵用暗号化
SD2
SD7
SD8
SD9
SD10
SD11
SD12
SD17
SD18
SD19
SD21
SD20
SD22
2 端末装置
情報センタ装置接続・情報要求
パスワード署名
検証データ生成
セッション鍵署名
セッション鍵暗号化
Session鍵、パスワード暗号化
情報蓄積部に蓄積
SD1
SD4
SD5
SD14
SD15
SD24
SD25
1 カード部
UID1
Cp
Di
Ki
入力部
23
情報蓄積部
29
PW
UID1
SD3
R
Cp(Di(PW)||R)
SD6
SD13
Di(Session)
Cp(Di(Session))
SD16
Session(情報本体)
SD23

【図11】


2 端末装置B
2 端末装置A
カード部
1
11
セキュリティ情報蓄積部
入力部
23
29
情報出力部
21
検証部
22
照合部
24
セッション鍵抽出部
署名生成部
25
公開暗号化部
26
慣用暗号化／復号部
27
情報蓄積部
28
20
通信制御部

【図12】



フロントページの続き

(72)発明者　高野　陸男
東京都千代田区内幸町１丁目１番６号　日
本電信電話株式会社内